TREND MICRO

Securing Your Web World



Can You Trust Your DNS?

Feike Hacquebord, Chenghuai Lu, Erik Wu
Advanced Threats Research, TREND MICRO

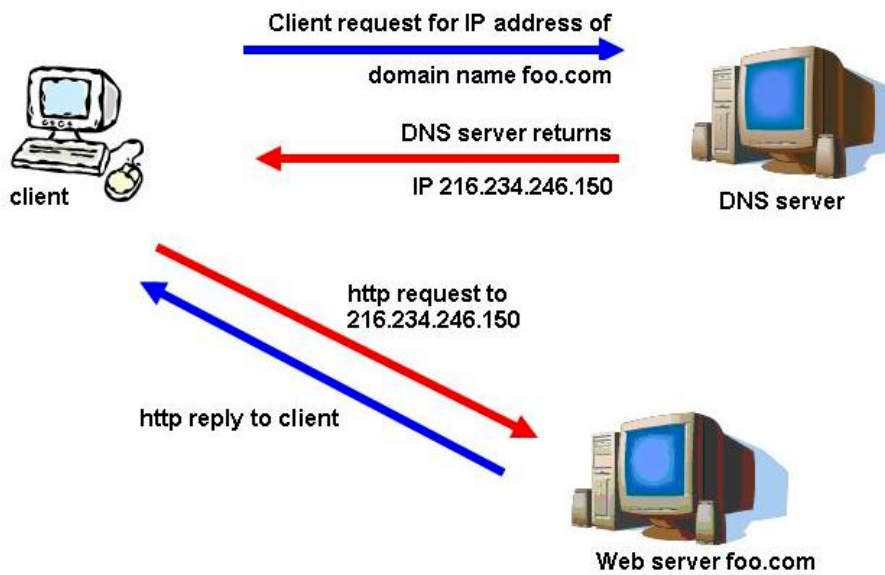
Virus Bulletin 2007
24/09/2007

Outline

- Introduction to DNS
- DNS Changer Trojans
- Rogue DNS servers
- A large network of rogue DNS servers related to Zlob
  - Hijacking of bad domain names
  - Clickfraud
  - Stealing personal information
- Automated detection of rogue DNS servers
- Remedies
- Conclusion

Introduction to DNS

- DNS (Domain Name System) servers translate human readable domain names to numerical IP addresses. This is essential for easy use of the internet.
- By default, most internet users use DNS servers of their ISP.
- DNS was not designed with security in mind. Internet users implicitly trust the DNS servers they use.



DNS Changer Trojans

- DNS Changer Trojans silently change DNS settings on the victim's computer to foreign DNS servers.
- An example are the fake Video Codecs (related to Zlob) which are spread with remarkable technological and social engineering tricks.
- Among the social engineering tricks are professional looking websites which try to lure internet users into installing a "codec" and even License Agreements…
- Some websites install a "unique" DNS Changer Trojan for each visitor (this was originally posted on a Unisog mailing list: http://lists.sans.org/pipermail/unisog/2006-November/026937.html)

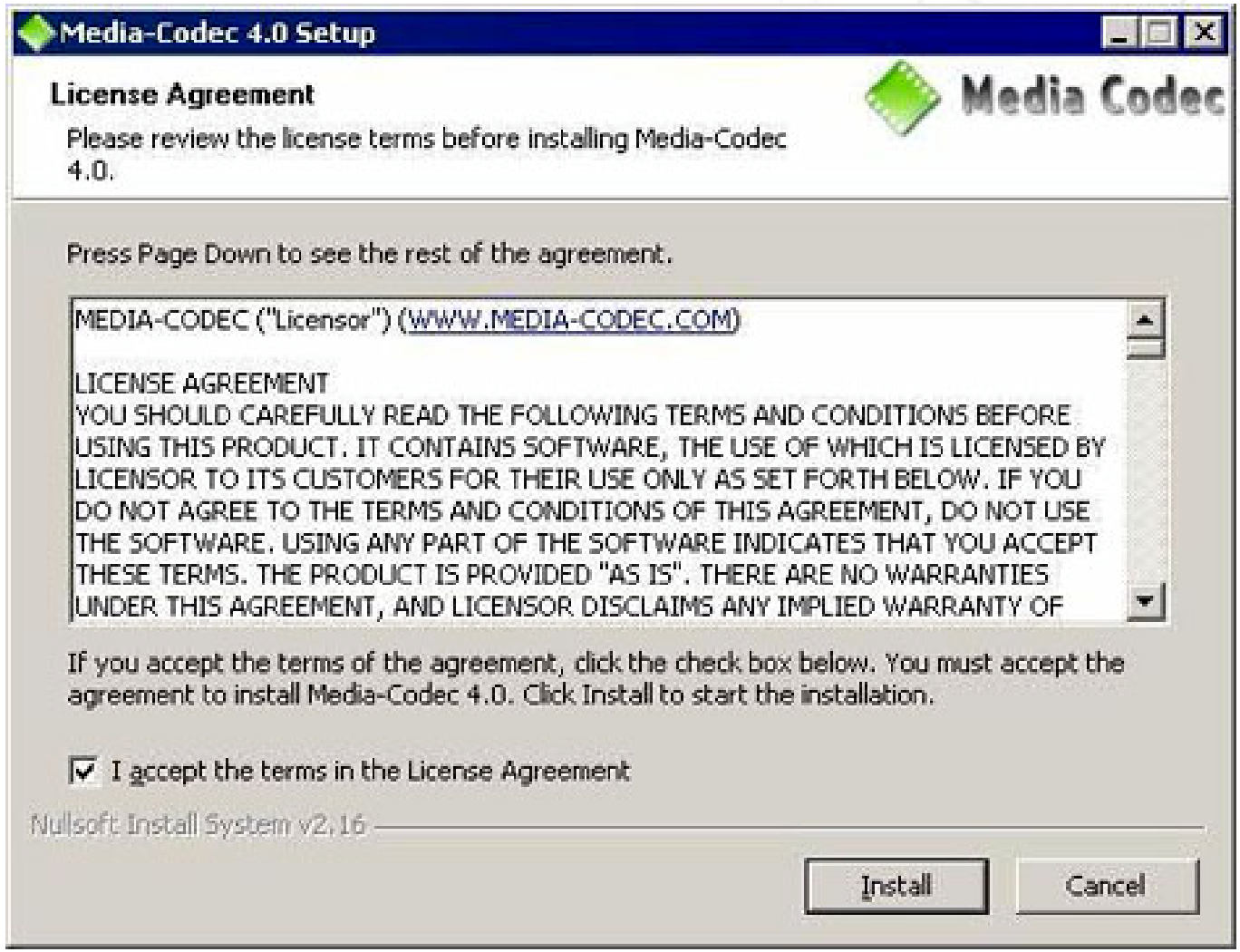
.

Website of a DNS Changer Trojan

- Professional looking websites attempt to lure internet users into installing a fake codec.

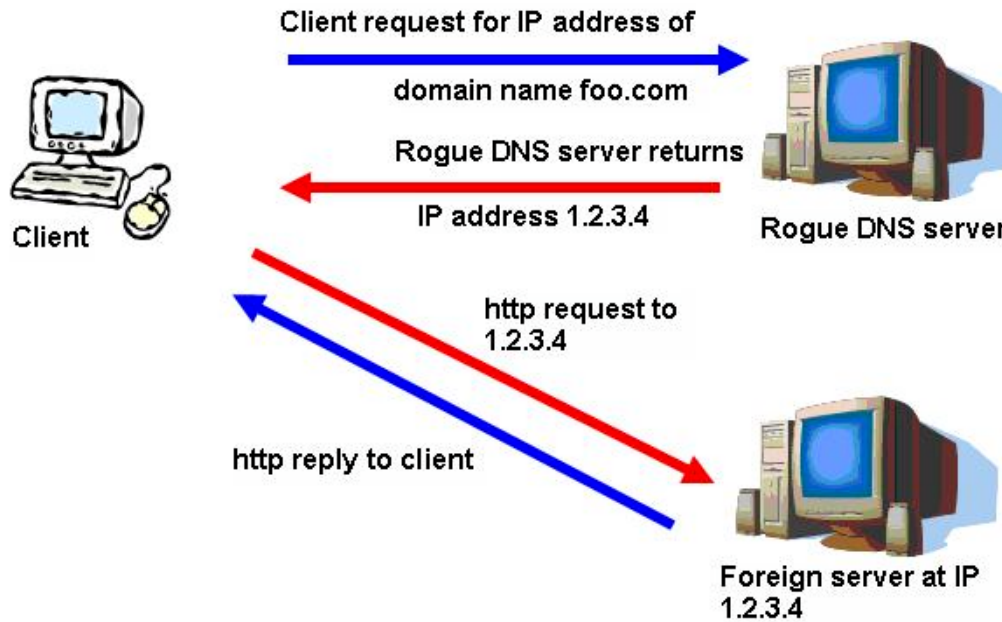
EULA of a DNS Changer Trojan

- A License Agreement of a DNS Changer Trojan



Rogue DNS servers

- Rogue DNS servers are controlled by untrusted third parties. They resolve certain domain names to fallacious IP addresses.
- Victims of rogue DNS servers may be directed to malicious websites without them noticing it.
- The surfing habits of victims of rogue DNS servers may be monitored for a long time. This makes targeted attacks possible.



Network of rogue DNS servers (Zlob related)

- We found more than 900 rogue DNS servers whose IP addresses are hard coded in DNS changer Trojans. These Trojans are spread by fake Video Codecs (Zlob related).
- These rogue DNS servers all exhibit the same kind of behavior.
- They get their internet connectivity from Intercage and Pilosoft
- This network is still expanding and about 2 years old.

Behavior of rogue DNS servers (Zlob related)

- Most domain names are resolved correctly.
- Non existent domain names get resolved. Victims are shown adult websites when they mistype a domain name in their browser.
- Domain names known for hosting malware and C&C servers are hijacked. Built-in update functions of other malware present on the victim's computers may lead to clicks on adult websites.
- Parked domain names are resolved differently. Instead of advertisements of parked domains other ads are shown.
- Sub domains of advertising companies are resolved differently. This leads to clickfraud.
- Sub domains of popular dating sites are resolved differently. This leads to leakage of personal information.

Hijacking a bad domain

- The Zlob network of rogue DNS servers hijack bad domain names of Trojans and C&C servers.
- Example: an old Trojan (year 2005) used to poll http://toolbarpartner.com/programs.txt for updates.
- The rogue DNS servers resolve toolbarpartner.com to 4 foreign IP addresses: 216.255.186.51, 216.255.186.59, 85.255.113.34 and 69.31.79.163.
- Send an HTTP request for the toolbarpartner.com URL to one of these IP addresses and you will get a very specific answer back → the old Trojan leads to automated clicks on adult websites.
- Apparently the 4 foreign IP addresses know about the *exact* URL which is being used by other malware to get updates!

Hijacking a bad domain (cont.)

- Apparently 216.255.186.51 knows the exact toolbarpartner.com URL used for updating a Trojan!

```
* Connected to 216.255.186.51 (216.255.186.51) port 80
> GET /programs.txt HTTP/1.1
> User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
> Accept: */*
> Host: toolbarpartner.com

< HTTP/1.1 200 OK
< Date: Mon, 17 Sep 2007 ..:..:.. GMT
< Server: Apache/1.3.34 (Unix) PHP/4.4.7 with Suhosin-Patch
< X-Powered-By: PHP/4.4.7
< Connection: close
< Transfer-Encoding: chunked
< Content-Type: text/html
http://toolbarpartner.com/1.exe
<html>
<head>
<title>Refresh Page</title>
</head>
<script>
top.location="http://69.50.190.131/?to=dname&from=in";
</script>
</html>
* Closing connection
```

Click fraud

- The Zlob related rogue DNS servers use a vulnerability in the setup of some advertising companies.
- Some advertising companies register clicks on several FQDNs. The Zlob related rogue DNS servers resolve a few of these FQDNs to foreign IP addresses and the other FQDNs correctly. The foreign IP addresses change ad tags in the URLs and then redirect victims to another FQDN of the advertising company which registers the click with the advertising tags changed.

- Targeted companies include: ccbill.com, fastclick.net, webpower.com, alexa.com, buy404s.com, penthouse.com, …

Click fraud (cont.)

- Example:
  - Refer.ccbill.com gets resolved to foreign IP 216.255.180.182
  - Ref.ccbill.com gets resolved to IP 64.38.240.20 (normal)

  - An infected user will load the advertisement link
    http://refer.ccbill.com/cgi-bin/clicks.cgi?CA=9235760000&PA=1472943&HTML=http://foo.com
    from foreign server 216.255.180.182. This foreign server changes the PA tag and then redirects the victim to
    http://ref.ccbill.com/cgi-bin/clicks.cgi?CA=9235760000&PA=1459740&HTML=http://foo.com

  - As a result the wrong party will be paid for showing the advertisement.

Information theft

- Dating sites of Friendfinder Inc have a similar vulnerability. Friendfinder accepts login data at two FQDNs.

- Zlob related rogue DNS servers resolve:
  - friendfinder.com to IP 216.255.180.130 (foreign)
  - **www**.friendfinder.com to IP 209.185.12.47 (normal)
  - IP 216.255.180.130 parses login data sent by victims to http://friendfinder.com/p/login.cgi and redirects victims to http://**www**.friendfinder.com/p/login.cgi with the login data -> leakage of personal information.

- Friendfinder claims to have ten millions of users.

Detection of rogue DNS servers

- Run DNS Changer Trojans in Sandboxing environment
- Look for changes in the Windows registry. In particular the registry value of *DhcpNameServer/NameServer*.
- Foreign IP addresses put in the Windows Registry by Trojans are probably rogue DNS servers.

Remedies

- ISPs can protect their internet users by
  - Dropping DNS queries to known rogue DNS servers
  - Detecting DNS queries to foreign DNS servers on the gateway
  - Forcing their customers to use the DNS servers of the ISP, much like forcing outgoing email to be relayed through the mail servers of the ISP.

Conclusion

- Rogue DNS servers are a major threat. They may be used for:
  - Click fraud
  - Theft of personal information
  - Targeted attacks
- The Zlob related rogue DNS network is
  - very large (900+ rogue DNS servers)
  - well connected to the internet
  - still expanding and at least 2 years old
  - … the bad guys must make a lot of revenue here …
- ISPs can protect their users by
  - blocking DNS queries to rogue servers
  - forcing their users to use the DNS servers of the ISPs

Thank You

Trend Micro | Securing Your Web World



TREND MICRO™